

## Wie man eine NIS 2 Gap-Analyse durchführt: Eine Checkliste mit Best Practices



Die Durchführung einer Gap-Analyse der NIS-2-Richtlinie erfordert sorgfältige Planung und Ausführung. Beachten Sie diese Best Practices bei der Planung Ihrer NIS-2-Gap-Analyse.



**1. Verstehen Sie die Anforderungen der NIS-2-Richtlinie:** Erwerben Sie ein tiefes Verständnis der Anforderungen der Richtlinie, um sicherzustellen, dass der Gap-Analyse-Prozess nicht nur effizient, sondern auch umfassend ist. Dies bedeutet, sowohl technische Spezifikationen als auch breitere organisatorische Maßnahmen genau zu prüfen.



**2. Definieren Sie die Ziele der Gap-Analyse:** Die Festlegung spezifischer Ziele wird einen klareren Rahmen für die Gap-Analyse bieten, die Bewertung leiten und die Entwicklung von sinnvollen Erkenntnissen und Maßnahmen erleichtern. Diese Ziele sollten mit Ihrer umfassenderen Compliance-Strategie abgestimmt sein.



**3. Führen Sie eine gründliche Lückenanalyse durch:** Überprüfen Sie systematisch bestehende Richtlinien und Verfahren, bewerten Sie die Wirksamkeit technischer Kontrollen und evaluieren Sie die Mechanismen zur Reaktion auf Vorfälle. Die Analyse sollte auch Ihre Praktiken im Bereich des Sicherheitsrisikomanagements und die Angemessenheit der Ressourcenzuweisung zu kritischen Bereichen der Cybersicherheit berücksichtigen.



**4. Bilden Sie ein spezialisiertes Team:** Stellen Sie ein interdisziplinäres Team zusammen, um ein umfassendes Verständnis Ihrer bestehenden Sicherheitsprotokolle sowie der Anforderungen der NIS-2-Richtlinie zu gewährleisten. Eine effektive Zusammenarbeit fördert die Konzentration auf die Analyseziele und unterstützt den Austausch von Erkenntnissen für einen effektiveren und strategischeren Plan zur Behebung identifizierter Mängel.



**5. Sammeln Sie relevante Dokumentationen und Daten:** Erfassen Sie bestehende Sicherheitsrichtlinien, Pläne für die Reaktion auf Vorfälle, Risikobewertungsberichte und alle weiteren relevanten Dokumente, die Ihre aktuelle Cybersicherheitslage widerspiegeln. Eine genaue und umfassende Datenerfassung legt eine Basis fest, gegen die Ihre Praktiken gemessen werden und stellt sicher, dass die Analyse auf Beweisen basiert. Dies ermöglicht eine präzise Identifizierung von Lücken zwischen den aktuellen Operationen und den Anforderungen der NIS-2-Richtlinie.

## Wie man eine NIS 2 Gap-Analyse durchführt: Eine Checkliste mit Best Practices



**6. Führen Sie eine Risikobewertung durch:** Eine umfassende Risikobewertung ermöglicht es Ihnen, die Sicherheit und Widerstandsfähigkeit Ihres Netzwerks und Ihrer Informationssysteme zu bewerten und die bestehenden Risiken und Schwachstellen zu identifizieren, die Ihre Konformität mit der NIS -2Richtlinie beeinträchtigen könnten. Durch eine gründliche Analyse der Risikolandschaft können Sie Bereiche priorisieren, die sofortige Aufmerksamkeit erfordern, und Ressourcen effektiv zuweisen, um die kritischsten Schwachstellen anzugehen.



**7. Identifizieren Sie aktuelle Sicherheitsmaßnahmen:** Dokumentieren Sie alle derzeitigen Sicherheitsmaßnahmen und Protokolle. Konzentrieren Sie sich darauf zu verstehen, wie diese aktuellen Sicherheitsmaßnahmen mit der NIS -2Richtlinie übereinstimmen, da dies spezifische Compliance-Lücken hervorhebt, die angegangen werden müssen. Sobald diese Lücken identifiziert sind, priorisieren Sie sie basierend auf dem Risikolevel, das jede für Ihre Organisation darstellt.



**8. Evaluieren Sie Compliance-Lücken:** Analysieren Sie die Lücken zwischen den Anforderungen der NIS 2 und den aktuellen Sicherheitsmaßnahmen Ihres Unternehmens. Diese Bewertung sollte die spezifischen Bereiche hervorheben, in denen Ihr Unternehmen die Standards der Richtlinie nicht erfüllt, und Klarheit darüber geben, was angegangen werden muss.



**9. Entwickeln Sie einen Aktionsplan:** Basierend auf den identifizierten Lücken erstellen Sie einen detaillierten Aktionsplan, der die Schritte und Ressourcen umreißt, die erforderlich sind, um diese Compliance-Lücken zu schließen. Dieser Plan sollte priorisiert werden, wobei die kritischsten Bereiche zuerst angegangen werden, um eine effektive Compliance mit der NIS -2Richtlinie zu gewährleisten. Der Aktionsplan sollte spezifische Ziele, Zeitpläne und verantwortliche Parteien für jede Aufgabe enthalten.



**10. Ergreifen Sie Abhilfemaßnahmen:** Setzen Sie den Aktionsplan um, indem Sie die notwendigen Sicherheitsmaßnahmen und Verbesserungen einführen. Dies kann die Einführung neuer Technologien, die Aktualisierung von Richtlinien und die Schulung des Personals umfassen, um die Einhaltung der NIS-2Richtlinie zu verbessern. Die Implementierung sollte eine koordinierte Anstrengung aller Beteiligten sein, um eine nahtlose Integration neuer Maßnahmen in bestehende Systeme zu gewährleisten.



**11. Überwachen und Überprüfen des Fortschritts:** Überwachen und überprüfen Sie regelmäßig den Fortschritt Ihrer Compliance-Bemühungen. Eine kontinuierliche Überwachung stellt sicher, dass die umgesetzten Maßnahmen wirksam sind und hilft dabei, neue Lücken oder Bereiche zu identifizieren, die weiterer Verbesserungen bedürfen. Die Nutzung von Schlüsselleistungsindikatoren (KPIs) und Metriken kann bei der Bewertung der Wirksamkeit der implementierten Änderungen helfen und sicherstellen, dass diese im Einklang mit der NIS-2-Richtlinie stehen.



**12. Dokumentation und Berichterstattung über Compliance:** Halten Sie detaillierte Dokumentationen aller Compliance-Aktivitäten und der vorgenommenen Verbesserungen fest. Die Dokumentation sollte den gesamten Umfang Ihrer Compliance-Reise erfassen und jeden Schritt des NIS -2Lückenanalyseprozesses von der Erstbewertung bis zur Umsetzung von Abhilfemaßnahmen detailliert darstellen. Aktualisieren Sie diese Dokumentation regelmäßig, um neue Entwicklungen zu berücksichtigen, und stellen Sie sicher, dass sie eine zuverlässige Ressource für interne Überprüfungen und externe Audits bleibt.

